White Paper

EdgeFort in the Enterprise

Extending Data Protection to the Edge of the Enterprise

Arkeia Software

Fall, 2007

EXECUTIVE SUMMARY

The enterprise data avalanche continues in a determined but irregular fashion. The key characteristics of data are changing, and so must data protection strategies of enterprises.

Large organizations must ensure that remote data and systems can be recovered when a disaster strikes. Six IT issues should be considered when evaluating remote office data protection solutions: security, reliability, scalability, serviceability, performance and integration.

The Arkeia EdgeFort backup and recovery appliance is designed to reduce the risks and costs of protecting remote office data. This white paper aims to show how EdgeFort is a low risk, low cost solution to the problem of rapidly growing distributed data.

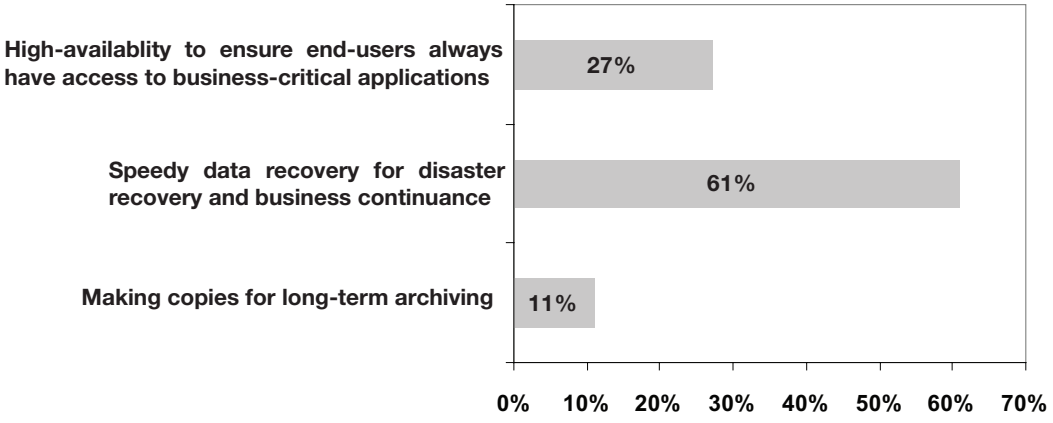
DATA AT 'THE EDGE'

It is apparent that remote offices and the data that they house are integral to business success. According to a 2007 Taneja Group and Storage Magazine study, 70% of respondents view remote sites as central to business operations. Another study, conducted by IBM, concluded that 93% of new data is being created at the edge of the enterprise (not in the data center). As the growth of remote office data and the corresponding need to protect that data is becoming an essential IT requirement, an overwhelming 75% of enterprises don't have IT resources in remote offices.

If the majority of new data is created at remote sites and the majority of those sites do not have local IT resources, how can enterprises be certain that all of their operational data is properly protected? Research shows that enterprises face three significant challenges associated with ROBO data management: ensuring speedy recovery, gaining control of data to mitigate risks, and controlling associated costs.

Ensure Speedy Recovery – regardless of what approach is selected to manage the ROBO data challenge, recovery of data is a critical objective. Backup and disaster recovery systems must be trusted to work and they must recover data quickly to avoid well documented costs of downtime.

PRIMARY OBJECTIVES OF REMOTE OFFICE BACKUP STRATEGIES



Source: Aberdeen Group

Gain Control of Distributed Data to Mitigate Risks - Whether data is consolidated at a central data center or secured in a remote site, IT Managers must be certain that the data is protected and accessible. Managing the risks associated with any IT solution is critical, but especially vital in large environments with many remote sites where a mistake could be compounded as it ripples through the distributed system. IT Managers must understand and manage risks to their infrastructure associated with security, scalability, performance and serviceability. It is also important to ensure overall fit with their IT plans. Risky, unproven technologies must be carefully evaluated.

Control Costs – given unlimited budgets, ROBO data protection options are plentiful. However, IT departments are under relentless pressure to do more with less, so the realities of current and planned budgets must be considered when selecting a solution. Optimal solutions should leverage existing investments (networking, infrastructure, training, etc.) and avoid the overpowered, risky and expensive solutions where they are not needed.

Remote Sites: Where to Keep the Data?

One of the most fundamental questions enterprises with remote data must answer is how much to consolidate to their data center versus keep at their local site.

In the Storage Magazine/Taneja Group survey of Storage Managers, 51% of organizations wanted to keep all or most of their IT resources deployed at the remote site and only selectively engage in consolidation. Further, only 16% indicated a desire to remove most/all of their IT resources from the remote site.

Source: Taneja Group and Storage Magazine

As the growth of remote office data accelerates, the corresponding need to protect that data is becoming an essential IT requirement.

INTRODUCING EDGEFORT

The Arkeia EdgeFort appliance product line is an all-in-one, federated data protection solution providing simple, reliable and affordable data protection for multi-site organizations. Ideal for large environments with distributed data, the EdgeFort Series is a powerful and scaleable, rack- mountable appliance. EdgeFort completely integrates Arkeia's award-winning network backup software and a complete backup hardware system, including disk and an optional integrated tape drive. EdgeFort's federated data management architecture allows remote and centralized data protection, making it possible for remote/ branch offices to backup, restore and archive critical data, with little or no local IT resource needed.

EdgeFort utilizes an all-new architecture capitalizing on directory based technology that allows enterprises to map data protection policies based on not only infrastructure but also hierarchical or geographical organization or any relevant criteria. The distributed architecture allows an enterprise to decide where

data should reside, to achieve the quickest backup and recovery: locally on disk, tape and/or production server or even remotely at the data center. The distributed architecture also eliminates the need to build out expensive bandwidth or hire local IT resources because data can remain local with central control.

EdgeFort comes standard with a remote management capability, allowing each appliance to be monitored, diagnosed and managed from a remote location such as an IT data center or enterprise NOC. Remote management reduces costs since there is no need to have a local IT resource to manage data protection. This feature makes management from a remote location as easy as local management. EdgeFort Central Management Server also enables central control of dozens or even hundreds of appliances so they can be managed from a single point. The Central Management Server improves control by providing better information via reporting on backup performance (backup window, disk and tape utilization, failed backups). Global data management policies can be implemented to ensure that corporate policy and/or legal or regulatory requirements are being met. Software update and upgrade of one, several or all EdgeFort appliances of an organization can be applied centrally, reducing maintenance costs.

The EdgeFort Series allows enterprises to gain control of data at the edge of the enterprise without having to invest in new network infrastructure, local IT or risky and expensive new technologies.

All EdgeFort appliances come bundled with hardware, software and maintenance, including:

- Arkeia Network Backup, robust highly-reliable, scalable data protection software for mid-sized and large networks.
- Unlimited licenses for network workstations & desktops, plus a limited number of server licenses
- Unlimited Encryption software to protect data from creation through destruction
- Virtual Tape Library and Disk-to-Disk-to-Tape management software
- Seamless integration with extensible options and agents to backup popular databases and applications such as Oracle, MySQL, MS Exchange and MS SQL servers
- Multiple hardware redundancies including swappable RAID drives, a hardened OS, and the application and OS on flash memory
- Completely redesigned Web 2.0 based user interface leveraging AJAX, making it easy to install, configure and manage
- 2 years of technical support, software updates, and hardware maintenance

The EdgeFort models vary in these ways:

EdgeFort 100 Series

- 2U desktop, small form factor, whisper quiet operation appliance
- 3 Server client licenses
- 250GB or 500GB usable capacity
- Optional integrated DAT72 or LTO2 tape drive; eSATA included

EdgeFort 200 Series

- 2U rack-mountable, scalable and powerful appliance

- 5 Server client licenses
- 500GB usable capacity, expandable to 1TB
- Optional integrated LTO2 drive; SCSI included

EdgeFort 300 Series

- 2U rack-mountable, scalable and powerful appliance
- 10 Server client licenses
- 1TB usable capacity, expandable to 2TB
- Multi-drive library option supported
- Integrated SCSI connection or integrated LTO2 drive

EDGEFORT IN THE ENTERPRISE

EdgeFort was designed from the ground up to support large, multi-site environments with distributed data and little or no local IT support. This approach has manifested itself in the final product in six main areas:

1. **Security –** data must support existing security investments and provide additional security to protect data at rest.
2. **Reliability –** backup and disaster recovery systems must be trusted to work.
3. **Scalability –** appliances must scale both vertically and horizontally.
4. **Serviceability –** hundreds of appliances must be as easy to manage as a single appliance.
5. **Performance –** backup window and recovery time objectives must be manageable for large amounts of distributed data.
6. **Integration –** appliances must slip seamlessly into an existing environment.

Analyst Take:
Brad O'Neil of the Taneja Group

"52% want to conduct backup operations in some combination of local and remote deployments. Again, this indicates that users want to maintain some resources at the edges of the organization. But why?

The answer is simple: The desire for selective consolidation reflects the realities about the requirements and management dispositions of firms. For many enterprises with larger remote sites or distributed workflows, maintaining significant ROBO IT resources is often highly desirable; there are often compelling availability or recovery reasons for keeping business-critical processes at least partially at the edge.

Resource consolidation technologies, while exciting and powerful, shouldn't be treated as a one-size-fits-all proposition. While WAFS and application-acceleration tools can transform distributed computing, it's clear their future will also require them to coexist with locally delivered and managed processes. **Users tell us their data will live on the edge of the enterprise for a long time."**

Security

Large enterprises must balance defense of their computing systems with keeping operations up and running to support business activities. Almost by definition remote data creates security concerns for enterprises. Due to it's configurable design, an EdgeFort implementation takes full advantage of existing enterprise security investments and adds a layer of new security to an infrastructure. The Edgefort OS is a security hardened, stripped down Linux operating system optimized for rapid backup and restore.

Availability - knowing that information can always be accessed. EdgeFort enables file backup to disk and/or tape to ensure rapid recovery and hence rapid access to information. Further, EdgeFort can be used as a full system bare-metal restore appliance, ensuring availability and access to critical enterprise systems.

Integrity - knowing that the information is accurate and up-to-date and has not been deliberately or inadvertently modified from a previously approved version. All EdgeFort appliances come bundled with the Arkeia Enterprise Encryption Option. This option encrypts data at the point of creation, at the client, therefore avoiding sending any unprotected data across the network (even an internal network). The data can stay encrypted through the appliance and onto tape to ensure that the integrity of the data is maintained from cradle-to-grave.

Confidentiality - knowing that sensitive information can be accessed only by those authorized to do so. The EdgeFort fully integrates with LDAP directory services to address common security issues such as authentication, directory integration, and server security integration. Further, EdgeFort management segments different roles (Admin, Operator, and User) which allow restriction of access to specific data by certain users. Role policy avoids internal risks due to unauthorized internal access and human errors caused by a lack of knowledge.

Due to the fact that the EdgeFort has a Linux-based OS it is less sensitive to viruses, Trojans, and other common security threats. EdgeFort's operating system allows security measures to be easily deployed and managed.

EdgeFort also authenticates all sending and receiving nodes prior to data transfer and utilizes only a single port. By using only a single port for communications, EdgeFort easily integrates into existing and/or new firewall policies.

EDGEFORT SECURITY SNAPSHOT

Objective	Description	Functionality
Availability	Knowing that data can always be accessed	**File Backup**: for rapid recovery and rapid access to information. **System Bare-Metal Restore**: ensuring availability and access to critical enterprise systems.
Integrity	Knowing that the information is accurate and up-to-date and has not been deliberately or inadvertently modified from a previously approved version.	**Encryption**: avoids sending any unprotected data across the network and ensures that the integrity of the data is maintained from cradle-to-grave. **Reporting**: granular details show data backup history.
Confidentiality	Knowing that sensitive information can be accessed only by those authorized to do so.	**Directory Integration**: leverages existing authentication, roles and server security decisions. **Role Management**: restricts access to certain data by certain users to avoid unauthorized internal access.

Reliability

Data protection is of no value if data backup and restore can not be trusted to perform when needed. EdgeFort has extensive hardware and software redundancies to ensure dependable operation. Hardware reliability is based on the selection of proven component suppliers, a best-in-class assembler, and appliance design decisions that optimize reliability.

Hardware reliability starts with proven component suppliers and manufacturers, so integrated in the EdgeFort are pre-tested and certified industrial class components to guarantee out-of-the box compatibility and operation. EdgeFort comes with a hardened Linux-based operating system to ensure the highest reliability and avoiding risks inherent to Windows-based systems. Moreover, the EdgeFort OS and backup software instance are stored on a flash card as an added layer of redundancy in case both disks fail.

Software reliability starts with the operating system and leverages the proven dependability of Arkeia's flagship backup software: Arkeia Network Backup. The EdgeFort OS was built from the ground up to work with the hardware. EdgeFort leverages various Arkeia Network Backup techniques to ensure a stable and efficient backup environment including:

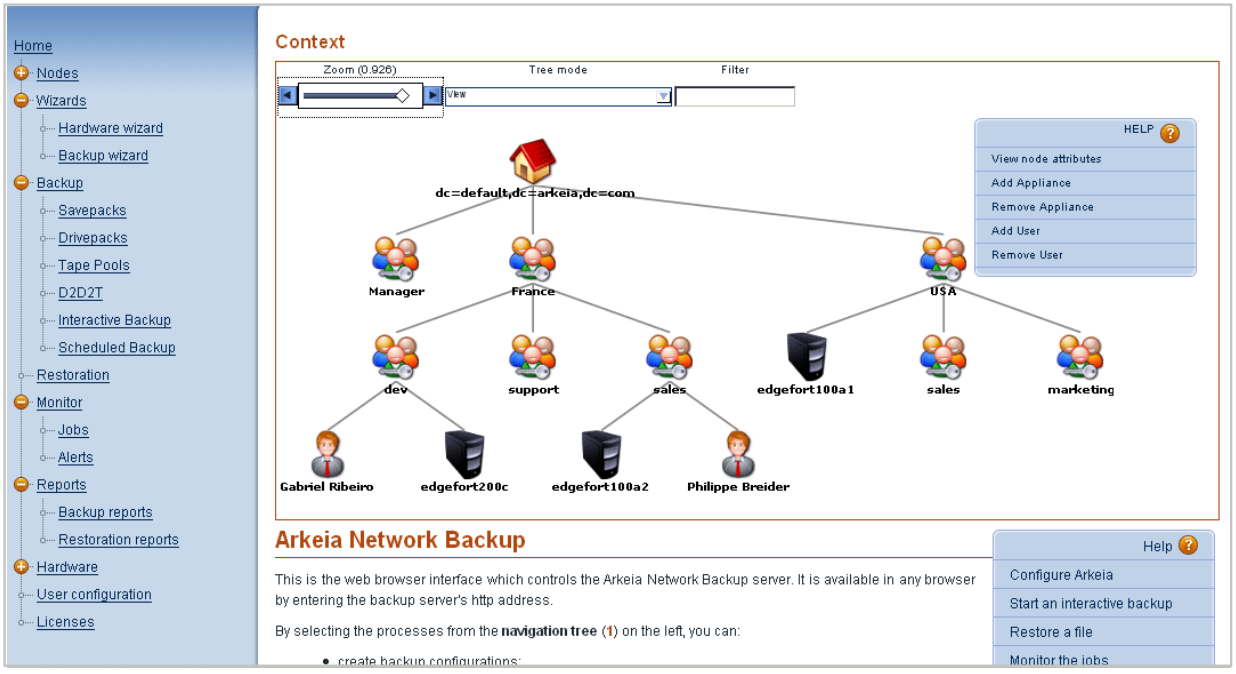
- Triple backup verification including (1) read/write verification on the client, (2) checksum between client and server, and (3) SCSI read/write verification.
- Arkeia Network Backup and its proven code base.
- Hardened lightweight Edgefort Linux-based OS utilizing the 2.6 kernel.

All of the hardware is pre-tested with the bundled software to ensure quick install and seamless operations. Finally, EdgeFort appliances come standard with better than industry average, two year hardware and software support and warranty.

Scalability

Well documented data growth requires a solution that can scale both horizontally and vertically. Solutions that have propagated across IT infrastructures without the capability of consolidated management end up creating more management headaches than they solve. EdgeFort's architecture is specifically designed to allow easy management of many appliances, so that fifty appliances are as easy to manage as one. This is perhaps the most distinguishing breakthrough of EdgeFort.

EDGEFORT GUI



Horizontal scalability allows an enterprise to start with just one EdgeFort, and add more to other locations as needed with little additional management overhead or complexity. The simplicity of adding units, transparency in managing them, and simple application of policies makes EdgeFort a good fit for enterprises with large amounts of widely distributed data. Multi-site administration means a global GUI or dashboard that informs IT of backup status, and a global policy engine that enforces

data protection policies across EdgeForts. Because EdgeFort leverages Web 2.0 communication architecture, a single EdgeFort Central Management Server can manage up to 200 EdgeForts simultaneously, with little network latency issues.

Vertical scalability was also a consideration in design of the EdgeFort, as data growth is rapid and often difficult to predict. A variety of EdgeFort models are offered to suit many environments. Today, the product line scales from 250GB of disk capacity up to 2TB. As disk capacities continue to increase, models are equipped with swappable and upgradeable drives. Additionally, with the option to add a tape library, vertical scalability often becomes more of a backup, retention and archive policy issue, rather than a hardware or appliance issue.

Performance

The time it takes to backup and restore files or recover from a system failure is a critical metrics when considering an enterprise-wide recovery solution. Leveraging the power of the Arkeia Network Backup engine, EdgeFort was designed to never be the bottleneck. Typically, the backup bottleneck will be determined by the speed of the tape device or the speed of the network. For instance, devices with the integrated LTO2 device may be limited to about 123GB per hour, the native throughput speed of the tape format. For disk only backup or restores, the performance limitation will likely be the speed of the network connection. Since external tape performance and network performance vary greatly in enterprises, the EdgeFort has been optimized to support the fastest environment.

EdgeFort utilizes various techniques to maximize performance and throughput including:

Parallelism: EdgeFort's performance is based, in part, on the number of simultaneous backup flows that are active at anytime. Each flow represents a client computer or a disk drive of a client computer. Parallel backup, or multi- flow, increases backup speed and reduces the overall time required to backup a group of networked computers by interleaving the data from several clients and disks at the same time. This allows for optimum network and tape drive usage even when the client computers are on different network loops and have different speed disk drives. The backup can be configured to use one flow per disk drive in the file servers and 1, 2 or even up to 200 flows for the entire group of desktop computers. This will backup the file servers very quickly and also backup the desktop pool in a reasonable period of time. When there are more clients or disks than flows, EdgeFort uses a round robin strategy, which can be modified, to complete the backup. As one client or disk completes its backup, the next available client or disk is started.

Cruise control: Dynamic, real-time bandwidth throttling allows administrators to reduce network congestion and optimize client processing priorities.

Client-side encryption & compression: EdgeFort encrypts and compresses data at the source, which reduces the backup window by leveraging the under-utilized processing power of client

machines rather than the backup server.

Integrated Virtual Tape Library: a fully integrated VTL with dynamic space allocation allows for flexibility, higher disk performance, and shortened backup and restore times.

Integration in Current Environment

One of the most difficult challenges companies face with their IT environment is integrating new technology with an existing infrastructure. Too many vendors assume their products are islands of their own, and do not consider the complications and implications of common enterprise environments. EdgeFort leverages the broad and deep support Arkeia Network Backup software has developed with more than 5,000 installations worldwide. EdgeFort is designed to painlessly fit into common enterprise environments, starting with one appliance and scaling to hundreds or thousands.

EdgeFort supports most major operating system as clients plus provides specific modules for hot backup of leading database and applications such as Oracle, MS SQL, MS Exchange, MySQL, etc. EdgeFort also leverages existing network investments (Ethernet, TCP/IP, etc.) and provides support for over 600 backup devices including autoloaders, libraries, and single tape drives. EdgeFort goes even further in supporting existing infrastructure investments by leveraging existing access control solutions. EdgeFort utilizes LDAP allowing it to integrate with other directory services such as Microsoft Active Directory, eDirectory, Sun One, and OpenLDAP.

EdgeFort can run side by side with existing backup solutions, and integrates directly with Arkeia Network Backup software so that enterprises who want to manage their own hardware in certain sites (the data center, for instance) can also centrally manage multiple EdgeFort appliances in their remote sites.

EdgeFort makes use of a centralized management model for controlling, configuring, scheduling, and monitoring other EdgeForts/backups. This allows EdgeFort to easily integrate into environments that have site-specific management requirements. Central management gives each appliance the ability to adhere to global and/or site specific policies, including:

- Ability to set site-specific or department-specific policies relevant to different types of required backup schema (for Marketing, Sales, Development, Support, etc.).
- Ability to set global policies or granular policies based on business requirements.
- Ability to get started with only one and grow only as needed.
- LDAP makes it possible to do user authentication and role management in a multi-site perspective. Role management can be based either on a customer's LDAP directory or on an EdgeFort provided one

Serviceability: Installation & Updates

Managing server and network infrastructure within the network operations centers of large enterprises is a challenge. However, managing the infrastructure that is distributed across remote branches and offices can prove to be even more complicated, time consuming and costly. With an increasing demand for high-availability environments, along with regulatory and commercial pressures, the issue of serviceability for the sites dispersed at the edge of the enterprise is becoming more and more important for the IT Manager. EdgeFort addresses these issues by leveraging centralized administration capabilities to manage and service multiple appliances.

The Central Management Server acts as a proxy to other appliances, both multiplexing commands from the GUI to other appliances and demultiplexing answers from appliances to the GUI. The interface is able to provide a combined view of all connected appliances. Such a management approach makes it possible to:

- Consolidate and centralize reporting information
- Deploy local and/or global policies
- Easily upgrade or configure multiple appliances
- Adhere to specific service requirements based on organizational needs

EdgeFort also addresses the issue of lack of control and standardization that is common in remote offices. Each EdgeFort appliance comes packaged with the same OS, same backup software, and same hardware, with the ability to configure the same policies. This decreases administration overhead, IT costs and risk of data loss.

EdgeFort is easy to install and update across hundreds or thousands of machines. The back-end infrastructure of EdgeFort will have the ability to deploy any kind of configuration relevant to any targeted appliances. All services can be launched on all appliances from the Central Management Server.

Finally, Operating System and backup software updates are also centrally managed. The backup software and the OS are a single entity. The software update package is downloaded from Arkeia's website to a desktop computer; from this computer, the customer uploads this package through the web GUI of the appliance to upgrade. From the Central Management Server the software update can be applied to multiple appliances at once.

CONCLUSION

The emergence of multi-site, distributed data growth within an enterprise calls for a remote office backup solution that not only protects data, but ensures overall business continuity. EdgeFort alleviates the complications associated with managing operations with distributed data by simultaneously ensuring the protection of desktop, laptop workstation, and server data in multiple locations. Although there are many approaches to solving the remote office/branch office (ROBO) data protection challenge, EdgeFort is the low risk, low cost solution for protecting the rising problem of rapidly growing distributed data.

To begin the first step in extending data to the edge of the enterprise, please call (888) 431-1319 or e-mail info@arkeia.com.

BEST PRACTICE DEPLOYMENT EXAMPLES

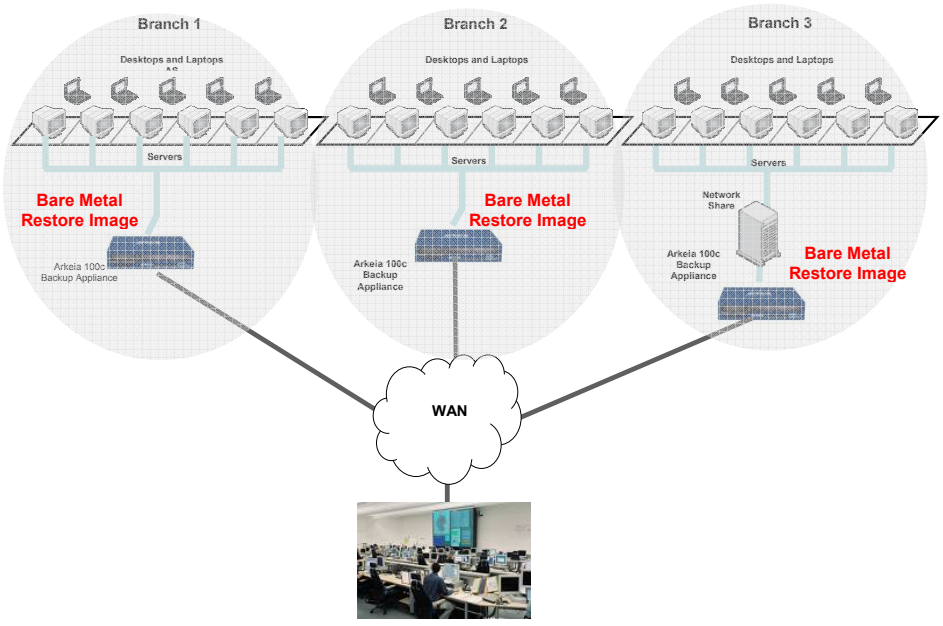
Scenario 1: Remote Office – Bare Metal Restore

While traditional file backup to disk and tape is a critical component of EdgeFort capabilities, another important use-case is the ability to do full system restores, or 'bare metal restore' of entire remote office systems. System restore differs from backup in two ways: first, unique system information (operating system, partition information, registries, passwords etc) are backed up, and second, the restore process involves automatically recovering an entire machine rather than a file or directory.

Often, restoring a remote office system requires days to complete, requiring new hardware, operating system image and configuration. With the EdgeFort at a local site, in the event of a failure, the restore process is performed quickly and efficiently to restore the system to its previous state without having to reinstall the OS, applications, system settings, partition information, and data. Once a new system is selected, central IT can recover the exact image of a failed machine over the network, directly from high-performing disk or tape. EdgeFort combined with Arkeia Disaster Recovery software simplified restoring a complete system including a complete recovery of the operating system, applications, system settings, partition information and data. Fast and easy restores save valuable recovery time during system failures.

Since the EdgeFort comes with disk and a tape option, both file backup and system backup can be securely stored on either media to meet recovery or archive objective. Each remote site can schedule a system backup for each of their critical servers at a remote site. The image can reside on either disk or tape at the location where it will most likely be needed and where it was created, at the remote office.

A typical topography may look like this:



In each branch office, a disk and tape EdgeFort is installed. Mission critical workstations are imaged and stored locally for rapid recovery. The image may be stored on an EdgeFort disk or tape. Supporting a bare-metal restore with an EdgeFort added allows for even greater remote office data protection, reduced risk and shorter time to recovery.

www.arkeia.com

Federated Data Protection